UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

IN RE: CBIZ DATA BREACH LITIGATION	Case No. 1:24-cv-1722-DCN **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Tina Fasano, Richard Giddings, and Chanelle Zimmerman ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Consolidated Class Action Complaint against Defendant CBIZ Benefits & Insurance Services, Inc. ("Defendant" or "CBIZ"), alleging as follows upon personal knowledge, information and belief, and investigation of counsel:

NATURE OF THE ACTION

1. This action arises from Defendant's failure to properly secure and safeguard Plaintiffs' and Class Members' sensitive and confidential personally identifiable information ("PII"), which as a result, has been disclosed to a notorious cybercriminal organization and published on the dark web.

2. From approximately June 1 through June 21, 2024, the notorious criminal ransomware group known as Meow Leaks accessed Defendant's network systems and stole Plaintiffs' and Class Members' PII stored therein, including their names, dates of birth, and Social Security numbers, causing widespread injuries to Plaintiffs and Class Members (the "Data Breach").

3. Defendant provides "financial and benefits and insurance services to organizations of all sizes, as well as individual clients," with "more than 120 offices and 6,500 team members" across the United States.[1]

4. Plaintiffs and Class Members are current and former employees of Defendant's clients, who, in order to obtain insurance and/or benefits serviced by Defendant, were and are required to entrust Defendant with their sensitive, non-public PII. Defendant could not perform its operations or provide the services it does without collecting Plaintiffs' and Class Members' PII. Defendant retains this sensitive PII for many years, even after the relationship between Defendant and Plaintiffs' and Class Members' employers has ended.

5. Businesses like Defendant that handle PII owe the individuals to whom the data relates a duty to adopt reasonable measures to protect such information from disclosure to unauthorized third parties, and has an ongoing duty to keep it safe and confidential. This duty arises under contract, statute and common law, in accordance with industry standards and representations made to Plaintiffs and Class Members, and because it is foreseeable that the exposure of PII to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to by the invasion of their private financial matters.

6. Defendant breached these duties owed to Plaintiffs and Class Members by failing to safeguard their PII that it collected and maintained, including by failing to implement industry standards for data security to protect against cyberattacks, which failures allowed criminal hackers to access and steal hundreds of thousands of current and former individuals' PII from Defendant's databases.

[1] CBIZ, Inc., https://www.cbiz.com/about-us/company-overview (last accessed January 8, 2025).

7. According to Defendant's notice to victims of the Data Breach ("Notice Letter"), "[o]n June 24, 2024, [Defendant] learned that an unauthorized party may have acquired information from certain databases." Defendant's ensuing investigation eventually determined "that an unauthorized party was able to exploit a vulnerability associated with one of [Defendant's] web pages, and acquired information from certain databases between June 2, 2024 and June 21, 2024." The exfiltrated data included files containing Plaintiffs and Class Members' PII.[2]

8. Plaintiffs have since discovered that the notorious Meow Leaks cybergang was behind the Data Breach and that, as of June 22, 2024, it posted the PII accessed therein on its dark web leak site. Any nefarious actor is now able to view, download, and use to commit further crimes against Plaintiffs and Class Members, including identity theft and fraud using their compromised and sensitive data.

9. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including Plaintiffs' and Class Members' names, dates of birth, and Social Security numbers.

10. Upon information and belief, current and former employees of Defendant's clients are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain employment or certain employment benefits offered by Defendant's clients. Defendant retains this information for many years after the relationship has ended.

[2] *See* Ltr., CBIZ, available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0dc5bcbc-8e0f-4825-be97-671405edd976.html (last accessed Jan. 2, 2025).

11. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

12. Defendant failed to adequately protect Plaintiffs' and Class Members' PII—and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its clients' employees' sensitive data.

13. Defendant maintained the PII in a reckless manner. In particular, PII was maintained on and/or accessible from Defendant's network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the PII left it in a dangerous condition.

14. Meow Leaks hackers targeted and obtained Plaintiffs' and Class Members' PII from Defendant's network because of the data's value in exploiting and stealing their identities. As a direct and proximate result of Defendant's inadequate data security and breaches of its duties to handle PII with reasonable care, Plaintiffs' and Class Members' PII was accessed by hackers and exposed to an untold number of unauthorized individuals. The present and continuing risk of identity theft and fraud to Plaintiffs and Class Members as victims of the Data Breach will remain for their respective lifetimes.

15. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact, including but not limited to (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred

mitigating the materialized risk and imminent threat of identity theft; (c) actual identity theft and fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their PII; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the continued risk to their sensitive PII, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect the PII it collects and maintains.

16. To recover from Defendant for these harms, Plaintiffs, on behalf of themselves and the Class as defined herein, bring claims for negligence, negligence *per se*, unjust enrichment, and invasion of privacy to address Defendant's inadequate safeguarding of Plaintiffs' and Class PII in its custody and its failure to provide timely or adequate notice to Plaintiffs and Class Members that their PII was compromised in the Data Breach.

17. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

18. Plaintiffs and Class Members seek compensatory damages, declaratory judgment, and injunctive relief requiring Defendant to (a) disclose, expeditiously, the full nature of the Data Breach and the types of PII exposed; (b) implement improved data security practices to reasonably guard against future breaches of PII in Defendant's possession; and (c) provide, at Defendant's own expense, all impacted Data Breach victims with lifetime identity theft protection services.

PARTIES

19. Plaintiff Tina Fasano is a natural person, and a resident and citizen of Reeders, Pennsylvania.

20. Plaintiff Richard Giddings is a natural person, and a resident and citizen of Lee's Summit, Missouri.

21. Plaintiff Chanelle Zimmerman is a natural person, and a resident and citizen of Montgomery, Pennsylvania.

22. Defendant CBIZ Benefits & Insurance Services, Inc. is incorporated under Missouri law with its principal place of business located in Cuyahoga County, Ohio.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class (for example, Plaintiffs Fasano and Zimmerman) is a citizen of a state different from Defendant.[3]

24. This Court has personal jurisdiction over Defendant because its principal place of business is in Ohio, and it engages in substantial and not isolated business in this state.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiffs' and Class Members' PII in this District, and has injured Class Members in this District.

[3] According to the Data Breach Notification submitted to the Office of the Maine Attorney General, 7 Maine residents were affected in the Data Breach. *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0dc5bcbc-8e0f-4825-be97-671405edd976.html (last accessed Dec. 23, 2024).

FACTUAL ALLEGATIONS

A. Defendant Owed Duties to Adopt Reasonable Data Security Measures for the PII it Collected and Maintained.

26. Defendant provides "financial and benefits and insurance services to organizations of all sizes, as well as individual clients," with "more than 120 offices and 6,500 team members" throughout the United States.[4]

27. Plaintiffs and Class Members are current and former employees of Defendant's clients, who, as a condition and in exchange for receiving insurance and benefits through their employers, were and are required to entrust Defendant with highly sensitive PII, including their names, dates of birth, and Social Security numbers.

28. In exchange for receiving Plaintiffs' and Class Members' PII, Defendant promised to safeguard the sensitive, confidential data and use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

29. At all relevant times, Defendant knew it was storing and using its networks to store and transmit valuable, sensitive PII belonging to Plaintiffs and Class Members, and that as a result, its systems would be attractive targets for cybercriminals

30. Defendant also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the individuals whose PII was compromised, as well as intrusion into those individuals' highly private information.

31. Upon information and belief, Defendant made promises and representations to its clients' employees, including Plaintiffs and Class Members, that the PII collected from them as a

[4] CBIZ, Inc., *Company Overview*, https://www.cbiz.com/about-us/company-overview (last accessed Dec. 23, 2024).

condition of obtaining services from Defendant would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

32. Indeed, CBIZ's Privacy Policy assures, "CBIZ takes reasonable measures to protect CBIZ-Collected PI (excluding public UGC), Client-service PI and Client-service PHI, from loss, theft, misuse and unauthorized access, disclosure, alteration, and destruction."[5]

33. Plaintiffs and Class Members reasonably relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

34. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard it. To that end, Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

35. Defendant derived economic benefits from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendant could not perform its operations, furnish the services it provides, or receive payment for those services.

36. By obtaining, using, and benefitting from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting that PII from unauthorized access and disclosure.

[5] CBIZ, Inc., *Privacy Policy*, https://www.cbiz.com/privacy-policy (last accessed Dec. 23, 2024).

37. Defendant had, and continues to have, a duty to adopt reasonable measures to keep Plaintiffs' and Class Members' PII confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of its IT networks and those of its vendors and affiliates.

38. Additionally, Defendant had and has obligations created by the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45 ("FTC Act"), 42 CFR part 2 ("Part 2"), common law, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and protected from unauthorized disclosure. Defendant failed to do so.

B. Defendant Failed to Adequately Safeguard Plaintiffs' and Class Member's PII, causing the Data Breach.

39. On or about August 28, 2024, Defendant began sending Plaintiffs and other victims of the Data Breach untitled Notice Letters about the Data Breach.

40. The Notice Letters generally inform as follows:

> **What Happened?** On June 24, 2024, we learned that an unauthorized party may have acquired information from certain databases. . . . Our investigation determined that an unauthorized party was able to exploit a vulnerability associated with one of our web pages, and acquired information from certain databases between June 2, 2024 and June 21, 2024.
>
> **What Information Was Involved?** We conducted a review of the data acquired and determined that the data included your name, Social Security number, and date of birth.[6]

41. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, the fact that the PII of Plaintiffs and other victims of the Data Breach was already for sale on the dark web, or an explanation of the remedial measures undertaken to

[6] A template Notice Letter is available at the website of the Maine Attorney General: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/-8e0f-4825-be97-671405edd976.html (last accessed Dec. 23, 2024).

ensure such a breach would not occur again. To date, these critical facts have not been clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII is protected.

42. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, then downloaded data from the networks and systems (a.k.a. "exfiltrated" data, or in layperson's terms "stole" data); and c) that once inside Defendant's networks and systems, the cybercriminals targeted most sensitive private information including Plaintiffs' and Class Members' Social Security numbers for download and theft.

43. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

44. Crucially, Defendant also failed to disclose in the Notice Letters that the notorious Meow Leaks hacker group was behind the Data Breach and had posted Plaintiffs' and Class Members' compromised PII on its dark web leak site.

45. Thus, Defendant's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

46. Meow Leaks accessed and exfiltrated Plaintiffs' and Class Members' PII in the Data Breach and published it to the Meow Leaks dark web link page in two tranches, on June 22

and July 16, 2024, where the PII has since been exposed to an untold number of bad actors with nefarious intentions.

47. Upon information and belief, Meow Leaks first breached Defendant's network and exfiltrated Plaintiffs' and Class Members' PII stored in un-encrypted form therein, using common and rudimentary initial access techniques that Defendant knew or should have known were necessary to protect against.

48. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiffs' and Class Members' PII, using controls like limitations on personnel with access to sensitive data and requiring multi-factor authentication ("MFA") for access, training its employees on standard cybersecurity practices, and implementing reasonable logging and alerting methods to detect unauthorized access.

49. For example, if Defendant had implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PII-collecting company is expected to employ—then Meow Leaks cybercriminals would not have been able to perpetrate prolonged malicious activity in Defendant's network systems for weeks without alarm bells going off, including the reconnaissance necessary to identify where Defendant stored PII, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

50. Defendant would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

51. Defendant did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiffs' and Class Members' PII it collected and maintained, such as encrypting files containing PII, requiring MFA for initial access to servers containing PII, or deleting PII from network systems when it is no longer needed, which caused that PII's unauthorized access and exfiltration in the Data Breach.

52. To mitigate cyber threats from ransomware gangs like Meow Leaks, the Joint Cybersecurity and Infrastructure Security Agency ("CISA") recommends rudimentary actions that businesses like Defendant should take: (a) installing updates for operating systems, software, and firmware as soon as they are released; (b) requiring phishing-resistant MFA (i.e., non-SMS text based) for as many services as possible; and (c) training users to recognize and report phishing attempts.[7]

53. Upon information and belief, Defendant failed to require phishing-resistant MFA where possible or adequately train its employees to recognize and report phishing attempts. Had Defendant required phishing-resistant MFA, and/or trained its employees on reasonable and basic cybersecurity topics like common phishing techniques or indicators of a potentially malicious event, Meow Leaks would not have been able to carry out the Data Breach.

54. Further, upon information and belief, Defendant failed to install updates for operating systems, software, and firmware as soon as they were released. Had Defendant installed such updates at its first opportunity as was standard and advised, the Data Breach would not have occurred or would have at least been mitigated.

[7] *#StopRansomware Guide*, CISA (Oct. 2023), available at https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf (last visited Oct. 24, 2024).

55. As a result of Defendant's failures, Plaintiffs' and Class Members' PII was stolen in the Data Breach when Meow Leaks hackers accessed and acquired files in Defendant's computer systems storing that sensitive data in unencrypted form.

56. Defendant's tortious conduct as detailed herein is evidenced by its failure to recognize the Data Breach at any point during the time cybercriminals roamed its network, accessing and exfiltrating Plaintiffs' and Class Members' PII, until the compromised data had already been published on the dark web, meaning Defendant had no effective means in place to detect, prevent, or stop cyberattacks.

57. As the Data Breach evidences, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive PII it collected and maintained from Plaintiffs and Class Members, such as encrypting the information or deleting it when it is no longer needed. These failures by Defendant allowed and caused cybercriminals to target Defendant's network and carry out the Data Breach.

58. Plaintiffs' and Class Members' PII was targeted, accessed, and stolen by cybercriminals in the Data Breach. Criminal hackers accessed and acquired confidential files containing Plaintiffs' and Class Members' PII from Defendant's network systems, where they were kept without adequate safeguards and in unencrypted form.

59. Defendant could have prevented this Data Breach by properly securing and encrypting the files and servers containing Plaintiffs' and Class Members' PII but failed to do so.

60. To make matters worse, Defendant waited over two months, until after Plaintiffs' and Class Members' PII was published on the dark web, to begin notifying them of the Data Breach or that they were affected. This unreasonable and unexplained delay deprived Plaintiffs and Class

Members of crucial time to address and mitigate the heightened risk of identity theft and other harms resulting from the Data Breach.

61. In the Notice Letters, Defendant offers 24 months of identity monitoring services, with less than 90-days to enroll. But this is wholly inadequate to compensate Plaintiffs and Class Members, as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

62. Defendant's offering of credit and identity monitoring establishes that Plaintiffs and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

C. Defendant Knew of the Risk of a Cyberattack because Businesses in Possession of PII are Particularly Vulnerable.

63. Defendant's negligence in failing to safeguard Plaintiffs' and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing such data.

64. PII of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the dark web.

65. PII can also be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This may be accomplished alone or in combination with other PII connected or linked to an individual, such as his or her birthdate, birthplace, and mother's maiden name.

66. Data thieves regularly target entities in the insurance technology industry like Defendant due to the highly sensitive information that such entities maintain. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

67. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[8] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[9]

68. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[10] Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry.[11] The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points.[12] The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.[13]

---

[8] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2020 23.pdf?hsLang=en (last acc. February 9, 2024).
[9] *Id.*, at 15.
[10] *See* Identity Theft Resource Center, *2023 Data Breach Report* (Jan. 2024), https://www. idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last accessed Dec. 23, 2024).
[11] *Id*.
[12] *Id.*
[13] *Id*.

69. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

70. Additionally, as companies become more dependent on computer systems to run their business,[14] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[15]

71. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[16]

72. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' PII compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

73. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network server(s), amounting to hundreds of thousands of

[14] Danny Brando, et al., *Implications of Cyber Risk for Financial Stability*, FEDS Notes (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last accessed Dec. 23, 2024).
[15] Suleyman Ozarslan, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, PicusLabs (Mar. 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed Dec. 23, 2024).
[16] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed Feb. 9, 2024).

individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the unauthorized exposure of that unencrypted data.

74. Plaintiffs and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

75. As a business and employer in possession of its clients' current and former employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiffs and Class Members due to a breach. Nevertheless, Defendant failed to take adequate measures to prevent the Data Breach despite knowing the risk such failure would cause.

76. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and the like.

D. Defendant Should Have Prevented the Data Breach, but Failed to Do So.

77. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing PII.

78. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[17]

79. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

[17] U.S. Gov't, *How to Protect Your Networks from Ransomware*, 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Dec. 23, 2024).

- Implement an awareness and training program. Since end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders

supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[18]

80. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

[18] *Id.* at 3-4.

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

81. Given that Defendant was storing the sensitive PII of its clients' current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

82. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of, upon information and belief, thousands to tens of thousands of individuals, including that of Plaintiffs and Class Members.

E. Defendant Knew or Should Have Known of the Risk Because Benefit-Administration Companies in Possession of PII are Particularly Susceptible to Cyber Attacks.

83. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they hold in custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

[19] *See* Microsoft Threat Intelligence, *Human-operated ransomware attacks: A preventable disaster* (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Dec. 23, 2024).

84. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

85. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

86. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

87. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

88. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to, upon information and belief, thousands to tens of thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

89. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

90. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

91. As a benefit-administration company in possession of its clients' employees' and former employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

F. Defendant was Required, but Failed, to Comply with FTC Rules and Guidance.

92. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

93. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

94. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

95. The FTC further recommends that companies not maintain confidential personal information, like PII, longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

96. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

97. Such FTC enforcement actions include actions against companies that fail to protect sensitive data like Defendant. *See, e.g., In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

98. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect sensitive personal information, like PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

99. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated

that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."

100. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

101. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

G. Defendant Failed to Comply with Industry Standards.

102. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

103. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.

104. In addition, the NIST recommends certain practices to safeguard systems, *infra*, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

105. Further still, CISA makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.

106. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04,

PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' PII, resulting in the Data Breach.

H. Defendant Owed Plaintiffs and Class Members a Common Law Duty to Safeguard their PII.

107. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiffs and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' PII.

108. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

109. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of PII in a timely manner.

110. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

111. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

112. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

113. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' PII from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights

I. Plaintiffs and Class Members Suffered Common Injuries and Damages Due to Defendant's Conduct.

114. Defendant's failure to implement or maintain adequate data security measures for Plaintiffs' and Class Members' PII directly and proximately caused injuries to Plaintiffs and Class Members by the resulting disclosure of their PII in the Data Breach.

115. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen fraudulent use of that information and damage to victims may continue for years.

116. Plaintiffs and Class Members are also at a continued risk because their Private remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect individuals' PII.

117. As a result of Defendant's ineffective and inadequate data security practices, the resulting Data Breach, and the foreseeable consequences of their PII ending up in criminals' possession and posted on the dark web, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent. Plaintiffs and Class Members have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d)

financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their PII; (g) loss of the benefit of their bargain with Defendant; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII it collects and maintains.

J. The Risk of Identity Theft to Plaintiffs and Class Members is Present and Ongoing

118. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

119. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[21]

120. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

[20] 17 C.F.R. § 248.201 (2013).
[21] *Id.*

121. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[22] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[23] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

122. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[24] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[25] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[26]

123. The unencrypted PII of Plaintiffs and Class Members has already been published on the dark web and will end up further sold and disseminated on the internet's black market

---

[22] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[23] *Id.*
[24] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[25] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[26] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

because that is the *modus operandi* of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Plaintiffs' and Class Members' PII.

124. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

125. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

126. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[27]

[27] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014),

127. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

128. The development of "Fullz" packages means that the stolen PII from this Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

129. Identity thieves can also use an individual's personal data and PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[28]

130. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of

https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Feb. 26, 2024).

[28] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

> goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[29]

131. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[30]

132. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[31] Yet, Defendant failed to rapidly report to Plaintiffs and the Class that their PII was both stolen and posted on the dark web.

133. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

134. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal

[29] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).
[30] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[31] *Id.*

Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card"; 4) Medical Identity Theft, and 5) Utility Fraud.[32]

135. According to the Social Security Administration, each time an individual's Social Security number is divulged, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other PII increases." [33] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[34]

136. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[35]

137. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[36] "Someone who has your SSN can use it to

---

[32] Alison Grace Johansen, *5 Kinds of ID Theft Using a Social Security Number*, LifeLock by Norton (Nov. 30, 2017), https://lifelock.norton.com/learn/identity-theft-resources/kinds-of-id-theft-using-social-security-number (last visited Dec. 23, 2024).
[33] *See* Soc. Sec. Admin., *Avoid Identity Theft: Protect Social Security Numbers*, https://www.ssa.gov/phila/ProtectingSSNs (last accessed Dec. 23, 2024).
[34] *Id.*
[35] Soc. Sec. Admin., *Identity Theft and Your Social Security number* (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 23, 2024).
[36] *See* Equifax, Inc., *How to Protect Yourself from Social Security Number Identity Theft*, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited Dec. 23, 2024).

impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[37]

138. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

139. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

140. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), *R&R adopted*, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to

[37] *See* Julia Kagan, *What Is an SSN? What to Know About Social Security Numbers*, Investopedia (Sept. 2, 2024), https://www.investopedia.com/terms/s/ssn.asp (last visited Dec. 23, 2024).
[38] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Dec. 23, 2024).

"impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.").

141. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[39]

142. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

143. In addition to out-of-pocket expenses that can exceed thousands of dollars, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

144. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

[39] *See* State of Calif. Dept. of Justice, *Your Social Security Number: Controlling the Key to Identity Theft*, https://oag.ca.gov/idtheft/facts/your-ssn (last accessed Dec. 23, 2024).

K. Loss of Time to Mitigate the Imminent Risk of Identity Theft and Fraud

145. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to (and even advised to) take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

146. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record.

147. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that harm.

148. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

149. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[40]

150. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches,

> law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

151. In other words, once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct and the resulting Data Breach.

L. Diminished Value of PII

152. Personal data like PII is a valuable property right.[42] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

---

[40] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).

[41] U.S. Gov't Accountability Off., *Report to Congressional Requesters* at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Dec. 23, 2024).

[42] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

153. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[43] For example, PII can be sold at a price ranging from $40 to $200.[44] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[45]

154. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, date of births, and names.

155. Such PII demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[46]

156. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[47] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information

[43] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Dec. 23, 2024).
[44] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Dec. 23, 2024).
[45] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Dec. 23, 2024).
[46] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10X Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 23, 2024).
[47] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[48, 49] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[50]

157. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

158. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

M. Reasonable and Necessary Future Costs of Credit and Identify Theft Monitoring

159. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach.

160. As foreseeable given the type of targeted attack in this case, the sophisticated criminal activity and type of information involved, and the *modus operandi* of cybercriminals, entire batches of stolen PII have already been published and disseminated on the dark web to criminals intending to use it for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or insurance, or filing false unemployment claims.

---

[48] https://datacoup.com/.
[49] https://digi.me/what-is-digime/.
[50] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

161. Such fraud may go undetected until debt collection calls start rolling in months, or even years, later. An individual may not know that his or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

162. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[51] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

163. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

164. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

PLAINTIFFS' INDIVIDUAL EXPERIENCES

Plaintiff Fasano

165. Plaintiff Fasano is a former employee at Sanofi Pasteur ("Sanofi"), which, upon information and belief, contracted with Defendant for services.

[51] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

166. As a condition of her employment at Sanofi, Plaintiff Fasano was required to supply Defendant with her PII, including but not limited to her name, date of birth, and Social Security number.

167. Plaintiff Fasano is very careful about sharing her sensitive PII. Plaintiff Fasano stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

168. At the time of the Data Breach—June 2, 2024 through June 21, 2024—Defendant retained Plaintiff Fasano's PII in its systems with inadequate data security.

169. Plaintiff Fasano received the Notice Letter, dated August 28, 2024, by U.S. mail, directly from Defendant. According to the Notice Letter, Plaintiff Fasano's PII, including her full name and date of birth, was improperly accessed and obtained by unauthorized third parties.

170. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff Fasano to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 months[,]" Plaintiff Fasano made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, contacting credit bureaus to place freezes on her accounts, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Fasano has spent significant on mitigation activities in response to the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

171. Subsequent to the Data Breach, Plaintiff Fasano has suffered numerous, substantial injuries including, but not limited to (i) invasion of privacy; (ii) theft of her PII; (iii) lost or

diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

172. Plaintiff Fasano's PII compromised in the Data Breach has already been misused, in that it has been published and disseminated on the Meow Leaks dark web leak site, which was directly caused by the Data Breach.

173. Plaintiff Fasano also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

174. The Data Breach has caused Plaintiff Fasano to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

175. As a result of the Data Breach, Plaintiff Fasano anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

176. As a result of the Data Breach, Plaintiff Fasano is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

177. Plaintiff Fasano has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Giddings

178. Plaintiff Giddings is a former employee at Sanofi, which, upon information and belief, contracted with Defendant for services.

179. As a condition of his employment at Sanofi, Plaintiff Giddings was required to provide his PII, including but not limited to his name, date of birth, and Social Security number, to Defendant.

180. Plaintiff Giddings is very careful about sharing his sensitive PII. Plaintiff Giddings stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

181. At the time of the Data Breach—June 2, 2024 through June 21, 2024—Defendant retained Plaintiff Giddings's PII in its system with inadequate data security.

182. Plaintiff Giddings received the Notice Letter, dated August 28, 2024, by U.S. mail, directly from Defendant. According to the Notice Letter, Plaintiff Giddings's PII,

including his full name, date of birth, and Social Security number, was improperly accessed and obtained by unauthorized third parties.

183. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff Giddings to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 months[,]"[52] Plaintiff Giddings made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, contacting credit bureaus to place freezes on his accounts, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Giddings has spent significant on mitigation activities in response to the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

184. Subsequent to the Data Breach, Plaintiff Giddings has suffered numerous, substantial injuries including, but not limited to (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

[52] Notice Letter, *supra*, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/-8e0f-4825-be97-671405edd976.html.

185. Plaintiff Giddings's PII compromised in the Data Breach has already been misused, in that it has been published and disseminated on the Meow Leaks dark web leak site, which was directly caused by the Data Breach.

186. Plaintiff Giddings also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of his PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

187. The Data Breach has caused Plaintiff Giddings to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

188. As a result of the Data Breach, Plaintiff Giddings anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

189. As a result of the Data Breach, Plaintiff Giddings is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

190. Plaintiff Giddings has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Zimmerman

191. As a condition of receiving insurance and/or benefits through an employer, Plaintiff Zimmerman was required to directly or indirectly provide to Defendant her PII, including but not limited to her name, date of birth, and Social Security number.

192. Plaintiff Zimmerman is very careful about sharing her sensitive PII. Plaintiff Zimmerman stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

193. At the time of the Data Breach—June 2, 2024, through June 21, 2024—Defendant retained Plaintiff Zimmerman's PII in its systems with inadequate data security.

194. Plaintiff Zimmerman received the Notice Letter, dated August 28, 2024, by U.S. mail, directly from Defendant. According to the Notice Letter, Plaintiff Zimmerman's PII, including her full name, date of birth, and Social Security number, was improperly accessed and obtained by unauthorized third parties.

195. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff Zimmerman to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 months[,]" Plaintiff Zimmerman made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach, contacting credit bureaus to place freezes on her accounts, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Immediately after receiving the Notice Letter, Plaintiff Zimmerman also spent time discussing her options with a law firm and has started to check her financial accounts for a minimum of thirty minutes per day in an effort to mitigate the damage that has been caused by Defendant. Plaintiff Zimmerman

has spent significant time on mitigation activities in response to the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

196. Subsequent to the Data Breach, Plaintiff Zimmerman has suffered numerous, substantial injuries including, but not limited to (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

197. Plaintiff Zimmerman's PII compromised in the Data Breach has already been misused, in that it has been published and disseminated on the Meow Leaks dark web leak site, which was directly caused by the Data Breach.

198. After the Data Breach, Plaintiff Zimmerman received a letter in the mail about a payday loan that she did not apply for. Plaintiff is concerned that someone used her PII from the Data Breach to obtain a payday loan in her name.

199. Plaintiff Zimmerman also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. Since approximately August or September 2024, Plaintiff Zimmerman has been receiving a combination of around 4-6 spam calls, texts, and many spam emails per day. Prior to this time, she was receiving maybe one troublesome call and/or email per day. This misuse

of her PII was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

200. Plaintiff Zimmerman is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from her and committing identity theft by way of a social engineering attack.

201. The Data Breach has caused Plaintiff Zimmerman to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence. Plaintiff Zimmerman is alarmed by the amount of her PII that was stolen or accessed, and even more by the fact that her Social Security number was identified as among the breached data from Defendant's computer system.

202. As a result of the Data Breach, Plaintiff Zimmerman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

203. As a result of the Data Breach, Plaintiff Zimmerman is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

204. Plaintiff Zimmerman has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches

CLASS ACTION ALLEGATIONS

205. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

206. The Class that Plaintiffs seeks to represent is defined as follows:

> **All individuals residing in the United States whose PII may have been accessed and/or acquired in the Data Breach, including all individuals who received a Notice Letter (the "Class").**

207. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

208. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

209. Numerosity. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

210. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the

questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct; and,

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

211. Typicality. Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

212. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

213. Adequacy. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

214. Superiority and Manageability. Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

215. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

216. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

217. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

218. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper

notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

219. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

220. Likewise, particular issues under Rule 23(c)(2) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant failed to timely notify the Plaintiffs and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard its clients' employees' PII; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

221. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 220 above as if fully set forth herein.

222. Defendant requires its clients' employees, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of providing its services.

223. Defendant gathered and stored the PII of Plaintiffs and Class Members as part of its business of soliciting its clients, which solicitations and services affect commerce.

224. Plaintiffs and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

225. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

226. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

227. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

228. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That

special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment with Defendant's clients.

229. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

230. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

231. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

232. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

233. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendant's possession had been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

234. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

235. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting benefit-administration companies in possession of PII.

236. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

237. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

238. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

239. Plaintiffs and the Class had no ability to protect their PII, which likely remains in Defendant's possession.

240. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

241. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

242. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

243. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

244. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

245. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' PII being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

246. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

247. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which

remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to implement adequate measures to protect the PII in its continued possession.

248. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

249. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

250. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and All Class Members)

251. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 220 above as if fully set forth herein.

252. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty. The Ohio Consumer Sales Practices Act ("CSPA") prohibits the same conduct. *See* R.C. 1345.01, et seq.

253. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of

failing to use reasonable measures to protect confidential data. The same duty arose under the CSPA, R.C. 1345.01, et seq.

254. Defendant violated the CSPA (as well as similar state statutes) and Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

255. Defendant breached its duties by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations, and;

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

256. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

257. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

258. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' PII being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

259. Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Class Members)

260. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 220 above as if fully set forth herein.

261. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their PII to Defendant. In exchange, Plaintiffs and Class Members should have had their PII protected with adequate data security.

262. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' PII for business purposes.

263. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

264. Defendant acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

265. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained employment at Defendant's clients.

266. Plaintiffs and Class Members have no adequate remedy at law.

267. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead

calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the security and the safety of their PII.

268. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

269. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' PII being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

270. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

271. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
INVASION OF PRIVACY –
PUBLICATION OF PRIVATE FACTS
(on behalf of Plaintiffs and the Class)

272. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 220 above as if fully set forth herein.

273. Defendant negligently or recklessly published Plaintiffs' and Class Members' PII to the public at large when it placed their PII on a web-accessible database that had a vulnerability permitting unauthorized public access.

274. Following the publication of Plaintiffs' and Class Members' PII on the unsecured web database, unauthorized third parties foreseeably accessed and exfiltrated this data to sell or use for criminal purposes.

275. The PII that was published (and later stolen) in the Data Breach is private and not of legitimate public concern. The disclosure of this PII is highly offensive to a reasonable person.

276. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs' PII being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII,

which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, pray for judgment as follows:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their undersigned Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide

to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its clients' employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps they must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees and costs as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury of all claims so triable.

Dated: January 8, 2025

/s/ Terence R. Coates
Terence R. Coates, Esq. (0085579)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
Email: tcoates@msdlegal.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC

227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
Email: gklinger@milberg.com

Jeffrey S. Goldenberg (0063771)
Todd Naylor (0068388)
GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Telephone: (513) 345-8291
Facsimile: (513) 345-8294
Email: jgoldenberg@gs-legal.com
Email: tnaylor@gs-legal.com

Gary E. Mason (admitted *pro hac vice*)
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com

Jeff Ostrow
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 332-4200
Email: ostrow@kolawyers.com

Attorneys for Plaintiffs and the Putative Class